AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF THE CLAIMS:

1. (previously presented) A method of operating a digital communication network having a plurality of nodes which have a locally hierarchical relationship, comprising the steps of:

supplying identification information at a first node to a transmission received from the network even if a sender of the transmission is not identified;

tracking network transmissions at the first node using the identification information and logging the identification information and a characteristic of the network transmission as traffic log information;

communicating the traffic log information to another node;

detecting a condition at the first node and communicating the condition to a trusted second node locally higher in said hierarchical relationship;

disconnecting one or more nodes in the network to test for the origin and scope of a potential attack and reconnecting disconnected nodes not associated with the potential attack;

collecting information regarding said condition and said traffic log through nodes at the same or higher hierarchical level as said trusted second node; and

controlling a response at said first node in response to said information, wherein the controlling step includes switching a critical segment of the network to a secure mode when a threat is detected, and wherein the hierarchical relationship of the plurality of nodes is hidden to users of the network.

2. (previously presented) A method as recited in claim 1, wherein said communicating of the traffic log and the condition is performed over said digital communication network separately from user data communications.

3. (original) A method as recited in claim 1, wherein said communicating and said controlling step are performed by user transparent communications over said digital network.

4. (original) A method as recited in claim 1, wherein said communicating and said controlling step are performed at bit rates of at least 10 Gbps.

5. (original) A method as recited in claim 2, wherein said communicating and said controlling step are performed preferentially to said user data communications.

6. (original) A method as recited in claim 1, wherein said controlling step establishes a virtual private network.

7. (original) A method as recited in claim 1, wherein said controlling step implements at least one of a mandatory access control policy and a discretionary access control policy.

8. (original) A method as recited in claim 1, wherein said communicating establishes a trust level for a node of said digital network.

9. (original) A method as recited in claim 1, wherein said communicating establishes a secure session between contiguous nodes of said digital network.

10. (original) A method as recited in claim 1, including the further step of detecting a foreign security policy manager connection.

11. (previously presented) A computer readable medium upon which is embodied a sequence of programmable instructions which, when executed by a processor, cause the processor to perform operations comprising:

detecting a condition at the first node and communicating the condition to a trusted second node locally higher in said hierarchical relationship;

disconnecting one or more nodes in the network to test for the origin and scope of a potential attack and reconnecting disconnected nodes not associated with the potential attack;

collecting information regarding said condition through nodes at the same or higher hierarchical level as said trusted second node; and

controlling a response at said first node in response to said information.

12. (previously presented) The computer program of claim 11, wherein the controlling step includes switching a critical segment of the network to a secure mode when a threat is detected.

13. (previously presented) The computer program of claim 12, wherein the secure mode is a virtual private network.

14. (previously presented) The computer program of claim 11, wherein the predetermined operations include the steps of:

supplying identification information at a first node to a transmission received from the network even if a sender of the transmission is not identified;

tracking network transmissions at the first node using the identification information and logging the identification information and a characteristic of the network transmission as traffic log information; and

communicating the traffic log information to another node.

15. (previously presented) The computer program of claim 11, wherein the hierarchical relationship of the plurality of nodes is hidden to users of the network.

16. (currently amended) A method of actively compartmentalizing a network in real time using manager objects and managed objects arranged in a locally hierarchically relationship, said method comprising:

providing a plurality of nodes, each node having at least one manager object and one or more managed objects, wherein each manager object corresponds to one or more managed objects and each managed object corresponds to a network connection to another node;

adding identification information to a transmission received at a first node from the network even if a sender of the transmission is not identified;

tracking network transmissions at the first node using the identification information and logging the identification information and a characteristic of the network transmission as traffic log information;

communicating the traffic log information to another node in a form that is transparent to users of the network;

detecting a condition at the first node and communicating the condition, in a form that is transparent to users of the network, to a trusted second node locally higher in said hierarchical relationship;

collecting information regarding said condition and said traffic log through nodes at the same or higher hierarchical level as said trusted second node;

controlling a response at said first node in response to said information; and

disconnecting one or more nodes in the network to test for the origin and scope of a potential attack and reconnecting disconnected nodes not associated with the potential attack.

17. (cancelled).

18. (previously presented) The method of claim 16, wherein the controlling step includes switching a critical segment of the network to a secure mode when a threat is detected.

19. (previously presented) The method of claim 18, wherein the secure mode is a virtual private network.

20. (previously presented) The method of claim 16, wherein the locally hierarchically relationship of manager nodes and managed nodes is hidden to users of the network.